

# ATSPI Technology Office

## Lightweight Portable Security (LPS) Public Edition (LPS-Public) User's Guide



The ATSPI Technology Office (AFRL/Rywa) was originally funded by the Department of Defense Research and Engineering Office under the Software Protection Initiative.

DISTRIBUTION A — Approved for public release; distribution is unlimited.

AFRL/Rywa

2241 Avionics Circle, Bldg. 620

Wright-Patterson AFB, Ohio 45433-7320

88 ABW-10-0024, approved 5 January 2010

# 1 Quick Start

For experienced users, here is the short version of how to get started using LPS:

1. Make sure your computer is configured to boot from a CD.
2. If using a wired Ethernet network, connect your computer to a network port.
3. Connect any external devices you will be using (hard drive, SmartCard reader).
4. Insert your CAC/PIV, if you want to visit CAC- or PIV-enabled websites.
5. Insert the LPS CD into the CD-ROM drive.
6. Boot the computer, verifying that LPS is loading.
7. If using a wireless Ethernet network, use the Network Manager utility to connect to it.
8. Launch Firefox and check that network connectivity exists.
9. Use the browser or run other loaded applications.

## 2 Introduction

Lightweight Portable Security (LPS), Public Edition (LPS-Public) is a hardened Linux client with a small memory footprint. It creates a pristine, trusted end-node within the volatile memory of an unmanaged computer system. LPS boots a small operating system from a CD-ROM without mounting the internal hard drive, thus bypassing any resident malware. Since a local hard drive isn't mounted, no persistent user session data is saved. Each time LPS boots, a trusted, known, read-only configuration is loaded.

LPS-Public can be used for many different situations where secure access is needed using untrusted systems:

- Minimizing the risk to corporate networks from untrusted computers (e.g., home computers, hotel business center PCs).
- Allowing secure remote access while controlling the outflow of data.
- Browsing the Internet without leaving traces of financial transactions, browser history, personal data, corporate information, or other private data on the host computer.
- Keeping personal data segregated from corporate data.
- Bypassing software keyloggers, persistent malware, or other rogue software.
- Allowing for fast, easy, low-cost continuity of operations (COOP) or business continuity.
- Quickly creating a secure end node using home computers of Government personnel.
- Allowing a single computer to be used in multiple roles while traveling, obviating the need to bring along multiple systems.
- Providing a “Plan B” for systems that are broken, locked-out, or are otherwise rendered unusable while traveling.

The standard LPS-Public distribution includes the Linux operating system, a CAC- and PIV-enabled Firefox web browser with Java and Flash support, Encryption Wizard, PDF viewer, a file browser, Remote Desktop Software (Citrix and Microsoft), SSH client, and the ability to use USB flash drives and portable hard drives. However, LPS can be customized for particular government or corporate missions and security requirements—including adding VPN clients and custom applications. This custom version is known as LPS-Remote Access, and is available for free to the US Department of Defense (DoD) and for a nominal fee to other US government agencies.

This User's Guide describes the features of the standard LPS-Public distribution and some of the most popular options. Please understand that not all features may be present in all versions of LPS. If you need features not present in your version of LPS, contact your computer support staff and request a customized distribution.

### 2.1 Using LPS to Improve Security

LPS differs from traditional operating systems in that it isn't continually patched. While this may seem like a disadvantage, it really isn't based on how LPS works. LPS is inherently more secure

than most operating systems since it is designed to run from read-only media and has no persistent storage. Any malware that might infect a computer can only run within that session. A reboot can clear any infection.

A user can improve security by rebooting between sessions, or when about to conduct a sensitive online transaction. For example, boot LPS immediately before performing any online banking activities. LPS should also be rebooted immediately after visiting any risky web sites, or when the user has reason to suspect malware might have been loaded. In any event, rebooting when idle is an effective strategy to ensure a clean computing session.

When using LPS on a USB flash drive, never use the LPS boot device as a data store. Use a separate flash drive for storing data. If your LPS boot stick is used as writeable storage, persistent malware could be loaded. LPS boots much faster from a USB flash drive than from a CD. If you intend to reboot frequently, running LPS from a boot stick can improve your experience.

LPS is updated on a regular basis (monthly patch releases, quarterly maintenance releases). Update to the latest versions to have the latest protection. When you launch Firefox, the default home page will be updated whenever you have an outdated version. Look for the red notice when a new version is available.

## 3 Getting Started

### 3.1 System Requirements

LPS has fairly limited requirements since Linux is not a resource-intensive operating system, and extraneous functionality has not been loaded. Basic LPS functionality requires:

- A computer system with an x86 processor. LPS is supported on standard Wintel-type PCs and Intel-based Macs.
- A minimum of 384 MB of RAM (LPS-Public, 512 MB or more recommended). For LPS-Public Deluxe, 640 MB of RAM (1 GB recommended).
- Ability to boot from CD-ROM (USB booting is also supported).
- Wired or wireless Ethernet connection (DHCP highly recommended).
- CCID-compliant USB SmartCard reader (if accessing CAC- or PIV-enabled websites).

LPS should work with all CCID-compliant, USB-connected SmartCard readers. Check data sheets or product documentation for the readers to determine if they support these standards. LPS has been extensively tested with the SCM SCR331 reader, one of the most common models within the DoD. Some readers require a firmware update for CCID compliance; a firmware updater is included within LPS for the SCR331 reader.

### 3.2 Hardware Setup

In order to run LPS, you must be able to boot from a CD or from a USB flash drive. The process is different on Macs and PCs due to architectural differences in the platforms. Be aware that Macs cannot easily boot Linux from USB flash drives, so only use LPS on a CD when using a Mac.

On a Mac, you can boot from a CD simply by holding down the “c” key during the boot process. If this approach does not work, boot your Mac normally then run the System Preferences utility in the Applications folder. Select Startup Disk. Choose the CD device, which may be labeled “Foreign OS on CDROM”, then restart the Mac. Note that this procedure requires administrator credentials.

On a PC, the process can be quite a bit more complicated. First, confirm that your BIOS boot priority lists the CD or USB drive *before* the internal hard drive. Often the easiest way to confirm this is to simply attempt to boot from the CD. If the LPS loading screen appears (Figure 1), you are booting from the CD. If your home operating system loading screen appears, you are booting from the internal hard drive. Some PCs provide a boot menu where you can make a one-time selection of the boot device; if you have a computer like this, you should select whichever device contain the LPS boot media (CD or USB).

If your PC is not configured to boot from CD by default, reboot the computer and enter the hardware setup screen. This usually involves pressing certain key(s) during a specific part of the boot process. The specific keys vary by hardware manufacturer and model, and are often a function key (e.g., F1, F2, F9, F10, or F12). The keys should be identified in the user’s guide for the computer, and are sometimes displayed on the screen during the boot process. Depending on

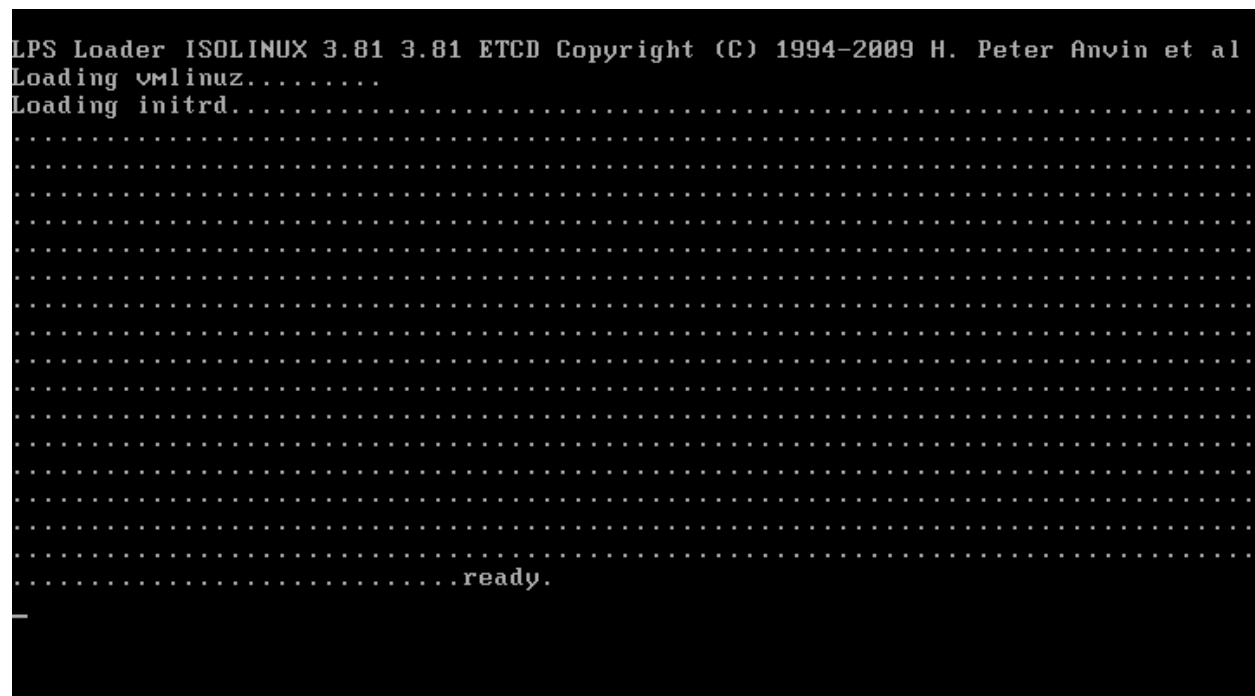
the speed of your computer and certain configuration settings, the interval where the setup key is recognized can be quite narrow. If the operating system on the computer's internal hard drive starts to load (e.g., if you see a Windows startup screen), you missed the interval where the key can be pressed—restart and try again.

If you intend to use wired Ethernet, connect your computer's Ethernet network port to a live network connection. LPS works best when the network uses the Dynamic Host Configuration Protocol (DHCP) service for assigning a unique network address to your computer. If you intend to use wireless Ethernet, you will configure this after LPS boots.

If you intend to use a CAC or PIV, connect the external SmartCard reader to an available USB port on your computer. Internal SmartCard readers are not fully supported. Insert your CAC or PIV into the SmartCard reader.

### 3.3 Starting LPS

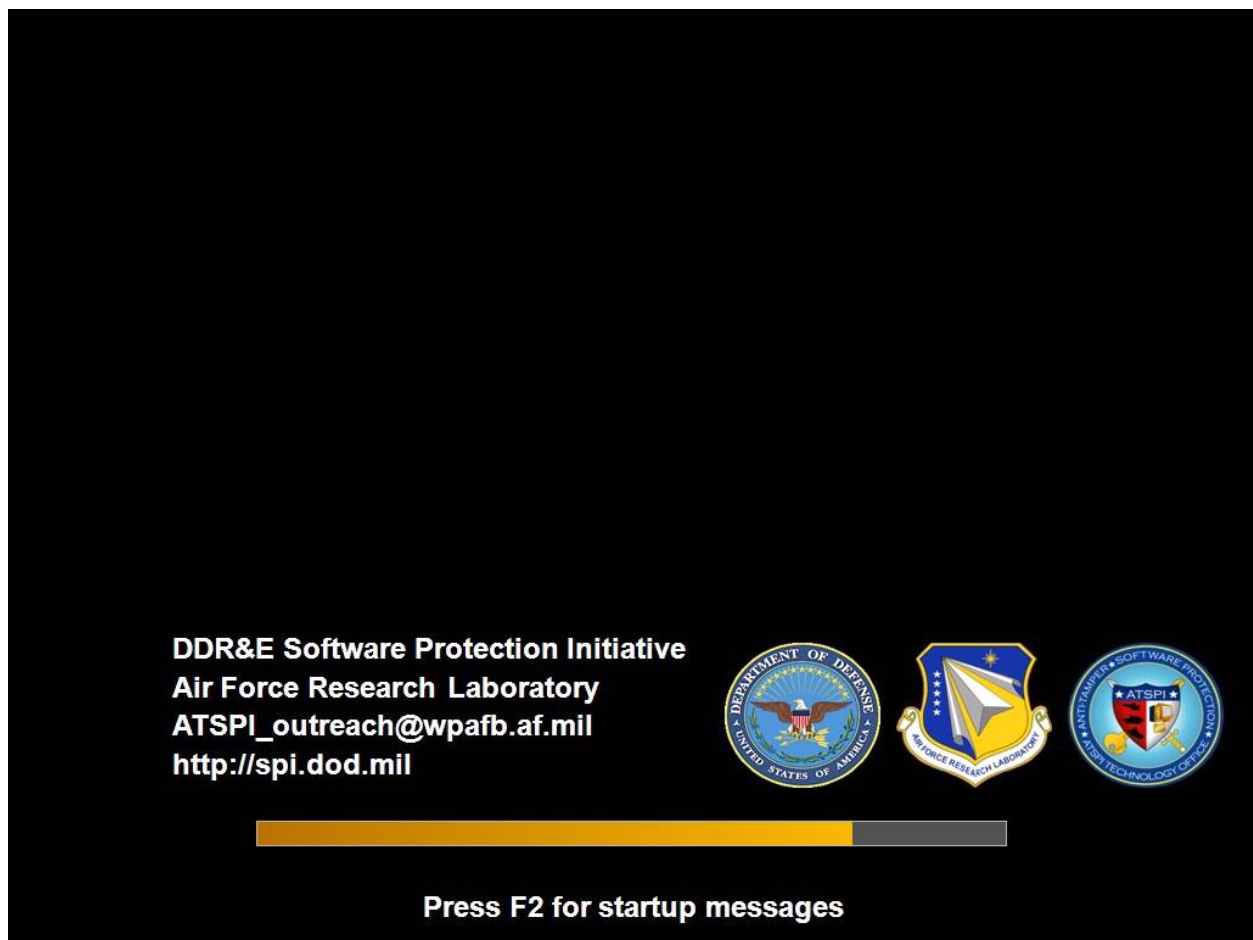
Place the LPS CD in your computer's CD drive or connect an LPS stick to an open USB port. Boot the computer. You should see the LPS loader screen, as shown in Figure 1:



### Figure 1 — LPS Loader Screen

LPS can take a few minutes to load since CD drives are typically much slower than hard drives. If you are booting from a fast USB memory stick, you can be ready to go in less than a minute.

After the loader screen, you will see the graphical user interface start and the Linux startup screen will display, as shown in Figure 2. The startup process can be monitored by observing the progress indicator bar on the startup screen.



**Figure 2 — LPS Startup Screen**

Pressing F2 during startup will display additional startup messages as individual processes start, as shown in Figure 3.

```
LPS init script



Loading modules:
pcmcia_core - serial_core - button - agpgart - intel-agp - nvidia-agp - yenta_socket - i82365 - tcic - 3c509 - 3c59x - 8139too -
8139cp - amd8111e - at1700 - cs89x0 - de4x5 - de2104x - depca - dmfe - hp100 - e100 - e2100 - eeepro - eeepro100 - eexpress - epi
e100 - eth16i - ewrk3 - fealnx - forcedeth - hp-plus - hp - lp486e - lance - ne2k-pci - natsemi - ni5010 - ni52 - ni65 - sis900
- smc-ultra - smc9194 - starfire - sundance - tlan - typhoon - tulip - via-rhine - wd - winbond-840 - xircom_cb - acenic - atl1
- atl1c - atl1e - atl12 - bnx2 - bnx2x - dl2k - e1000 - e1000e - ns83820 - r8101 - r8168 - r8169 - sis190 - skge - sky2 - tg3 - v
ia-velocity - tun - 3c589_cs - 3c574_cs - fmvj18x_cs - pcnet_cs - nmclan_cs - smc91c92_cs - xirc2ps_cs - axnet_cs - ibmtr_cs - a
iro_cs - atmcl_cs - netwave_cs - orinoco_cs - orinoco_nortel - orinoco_plx - orinoco_tmd - ray_cs - wavelan_cs - wl3501_cs - air
o - ath5k - ath9k - at76c50x-usb - atmcl_pci - adm8211 - wl - ipw2100 - ipw2200 - iwlagm - iw13945 - libertas_cs - libertas_sdio
- mw18k - orinoco_pci - rndis_wlan - rt2400pci - rt2500pci - rt2500usb - rt2800pci - rt2800usb - rt61pci - rt73usb - rt18180 -
rtl8187 - usb8xxx - zd1211rw - arc4 - aes-i586 - michael_nic - ieee80211_crypt_wep - ieee80211_crypt_tkip - ieee80211_crypt_ccmp
- lib80211_crypt_wep - lib80211_crypt_tkip - lib80211_crypt_ccmp - b44 - cdc-acm - usbhid - usb-storage - sr_mod - ide-cd_mod -
ata_piix - isofs - vfat - ntfs - ext3 - ac - battery - fan - processor - thermal - 8250 - 8250_pci - 8250_pnp - ehci-hcd - ohci
-hcd - uhci-hcd - sd_mod - nls_cp850 - nls_iso8859-1 -

Initializing rc0 packages...
profile_setup - secure - pcmcia - network -

Configuring and Starting Loopback interface...
acpi - network_files - crond - syslogd - pkg - filesystem_network - profile_setup - bootmenu - pcsd - session - menu - opensc -
playcd - rdate - sh - snmp - telnetd - console-keymap - audio - dbus - wicd - nimeinfo -

Initializing rc5 packages...
xorg-intel - xorg7-nv - xorg7-radeon - firefox.init - hwclock - ica.init - icewm.init - sound-nasd - ssh.init - x - xorg7-nvidia
- xorg7-vmware - pcmanfm - _
```

**DDR&E Software Protection Initiative**  
**Air Force Research Laboratory**  
**ATSPI\_outreach@wpafb.af.mil**  
**<http://spi.dod.mil>**

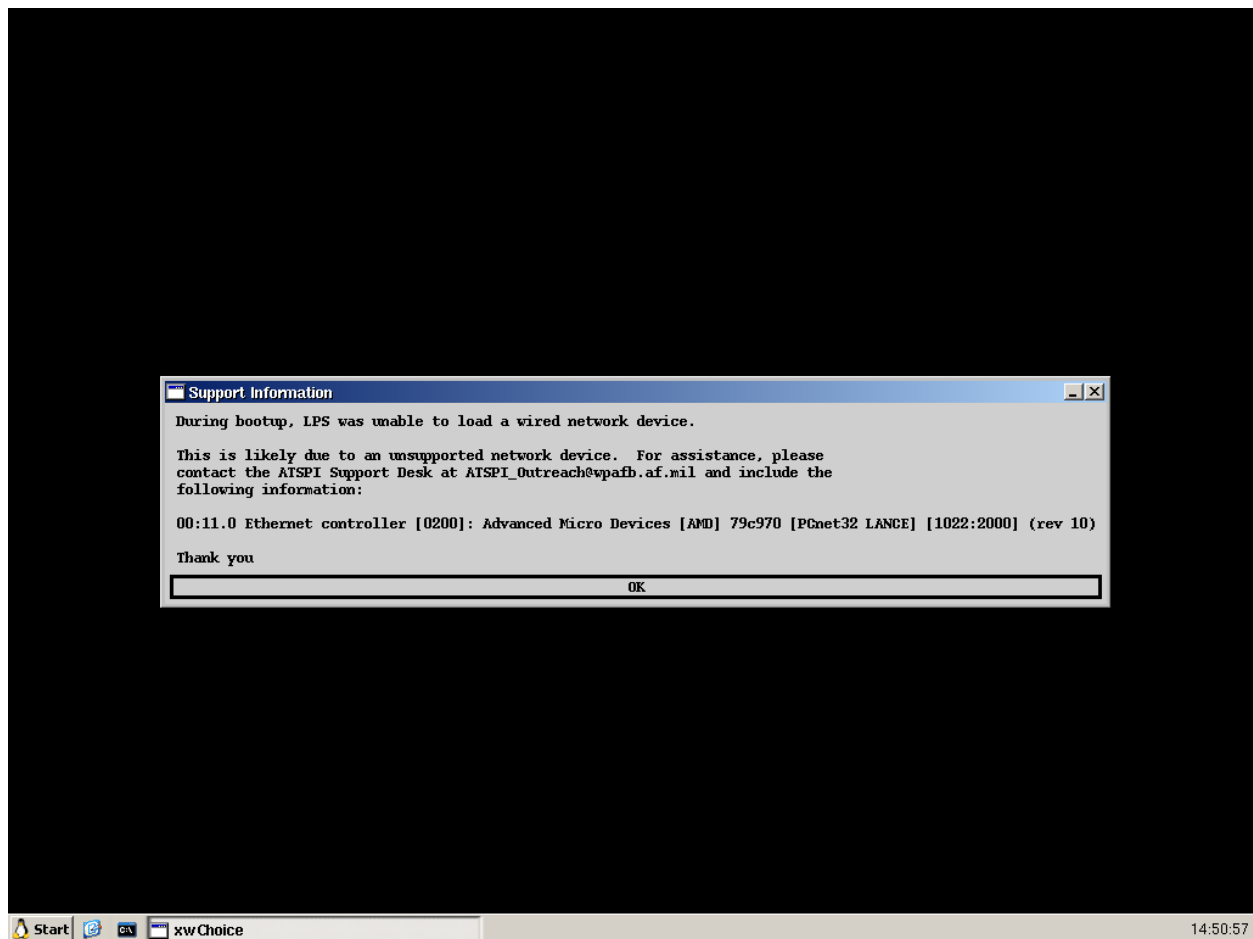




**Figure 3 — LPS Startup Screen (Verbose)**

However, this is not required and the computer will continue to start without pressing F2. The process can be monitored by watching the progress indicator bar on the startup screen. The verbose startup screen can be used to diagnose any problems with the startup process.

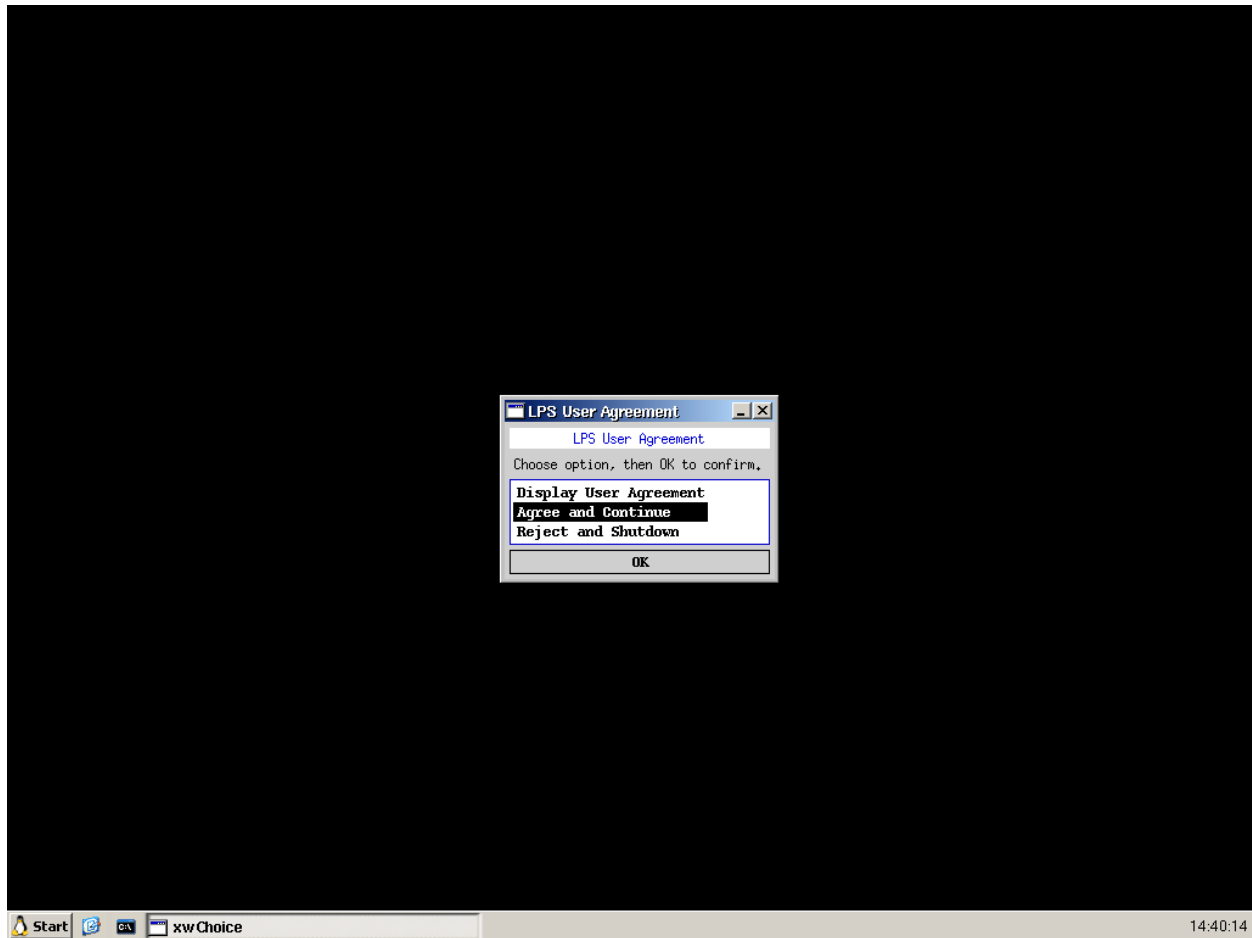


If a wired network device is detected but that device does not have an associated network driver, the screen shown in Figure 4 will display. This means that your computer has a network card that isn't recognized by LPS. You may still be able to use LPS if you have a wireless interface, but we would still like you to report this error to us.



**Figure 4 — Network Connection Not Detected**

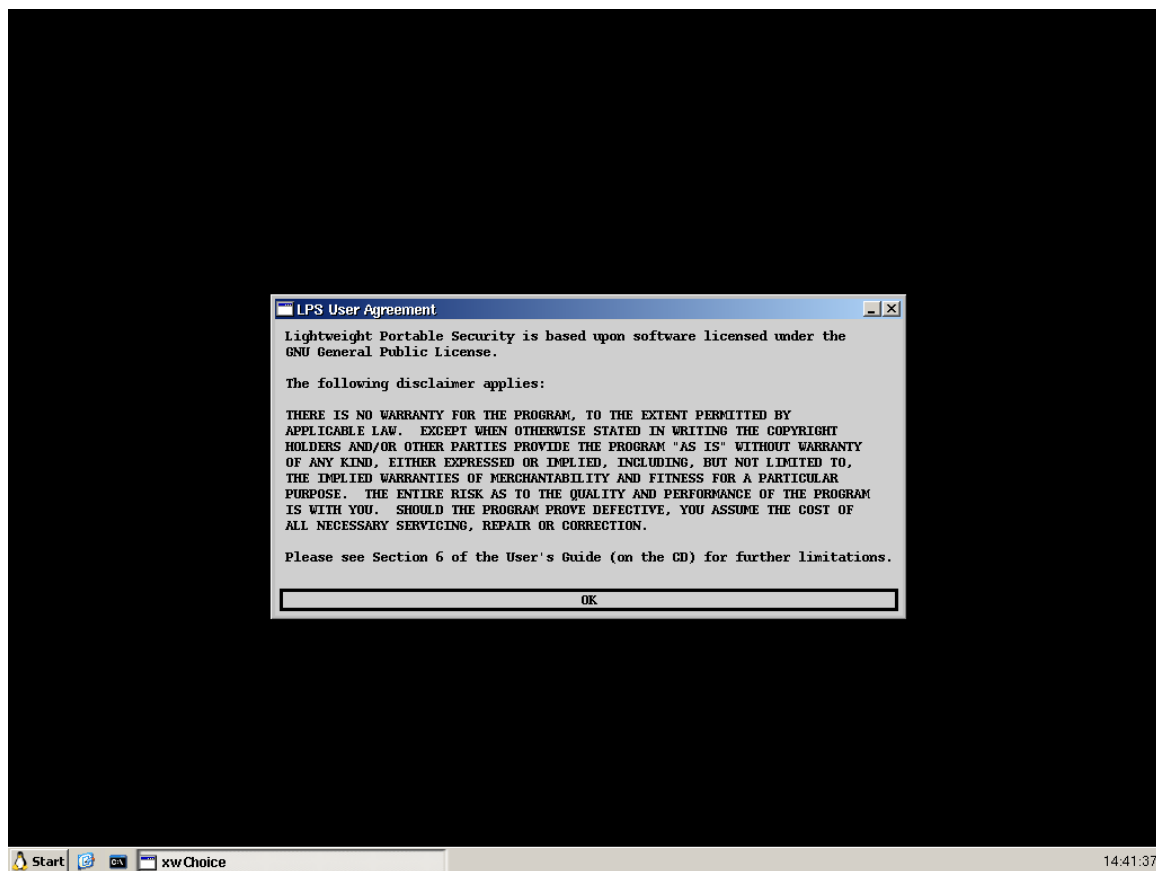
Once LPS is booted, but before it is available to use, the user will be prompted to accept the User Agreement, as shown in Figure 5.



**Figure 5 — LPS User Agreement Screen**

If the user agreement is accepted, the loading process will continue and the LPS desktop will be presented.

If the user agreement is rejected, the loading process will stop, the LPS disc will be ejected or the USB stick will be unmounted, and the computer will shut down. If you choose the option to display the User Agreement, you will be presented with the screen as shown in Figure 6.



**Figure 6 — LPS User Agreement**

If LPS was booted from a USB stick, LPS will automatically unmount the device and show the warning message in Figure 7. This is a security precaution to prevent the boot device from being modified. Re-inserting the stick will allow it to be mounted, but we recommend using a separate data stick for any user files. This is the safest method for using LPS with a USB stick.



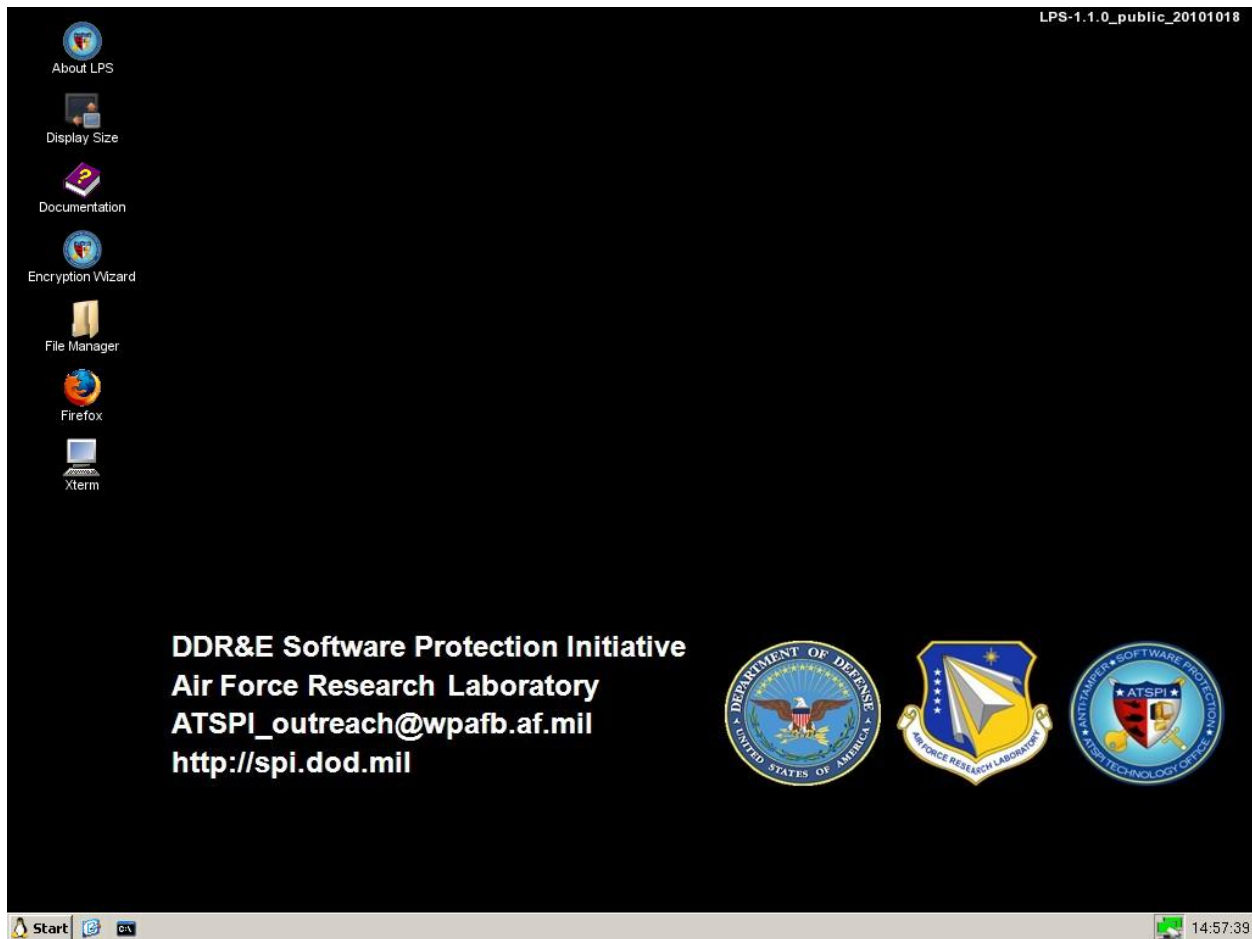
**Figure 7 — USB Boot Device Unmounted**

## 4 Using LPS

LPS-Public is our flagship product and contains core features most needed by the widest range of our customers. We do create custom builds for specific organizations, so not all features and screens described in this guide will be the same in all distributions.

### 4.1 The LPS Desktop

Once the startup process finishes, you will be presented with either the LPS-Public desktop shown in Figure 8 or the LPS-Public Deluxe desktop shown in Figure 9.



**Figure 8 — LPS-Public Desktop**

This is the LPS-Public desktop environment. If you are running a customized distribution, your desktop may look different. This desktop contains icons for:

- About LPS — the “about box” describing the program
- Display Size — the LXRandR utility to change the screen resolution
- Documentation — online documentation for LPS, including Frequently Asked Questions
- Encryption Wizard — ATSPI’s file encryption program

- File Manager — a GUI-based file browser (PCMan File Manager)
- Firefox — a popular web browser with CAC/PIV, Java, and Flash support, and several useful add-ons
- Xterm — a terminal emulator for the X Window System (provides local command line access to Linux)

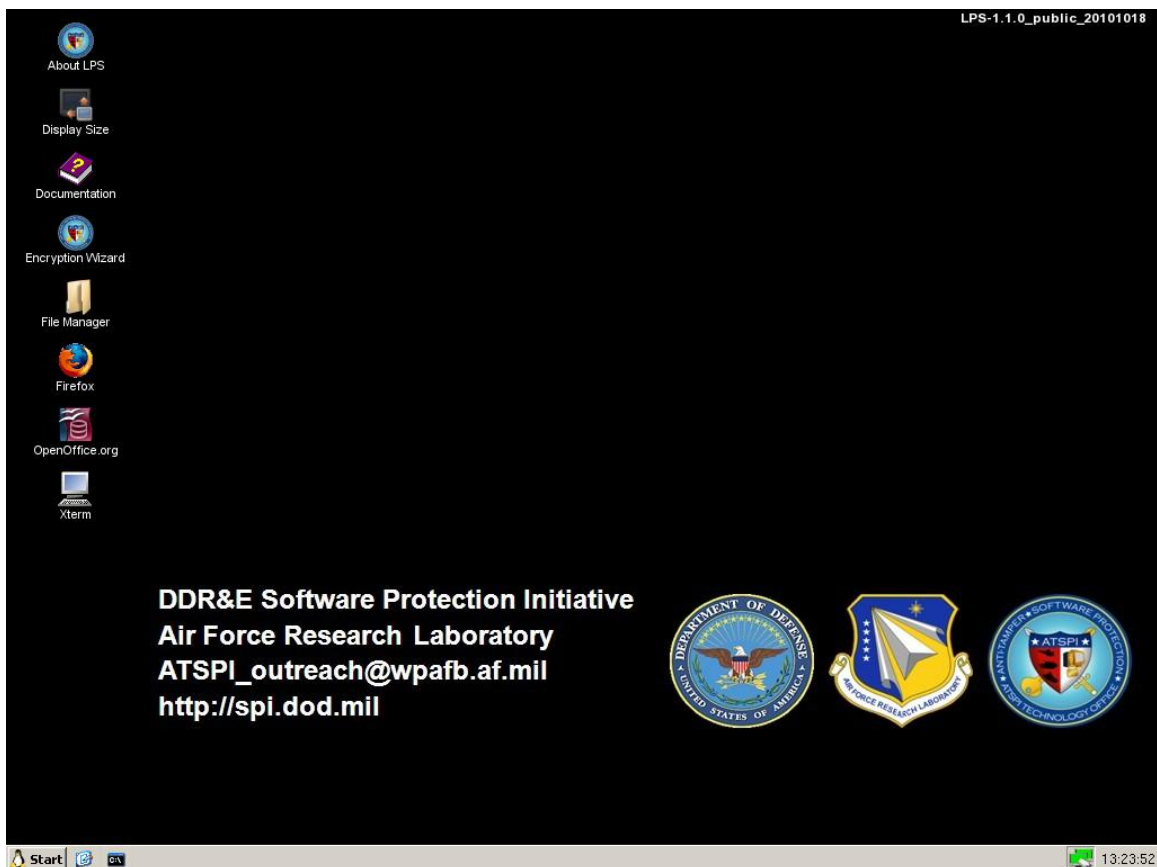
Optional icons that only are present under certain circumstances:

- NVIDIA Display Settings — an advanced utility for adjusting details of your display. This icon is only displayed if your system contains an NVIDIA brand display adapter (graphics card or chipset).
- OpenOffice.org — only available in LPS-Public Deluxe, this is the starting point for opening Open Office applications.
- USB Device [sda1] — a shortcut to the first attached USB drive (sda1); any other attached devices would show up in a similar manner with a different drive name (sdb1, sdc1, etc.). This icon only appears when a USB storage device is mounted.

The status bar at the bottom of the screen has several areas containing useful utilities and information.

- The Start Button provides quick access to the same programs shown as icons on the desktop, along with other important but infrequently-used utilities.
  - The Connectivity folder contains networking utilities:
    - Network Manager — the wicd network manager, which allows configuration and selection of wired and wireless connections.
    - Citrix Receiver — the Citrix Receiver client, allowing connection to Citrix servers using the ICA protocol.
    - Remote Desktop [full] — the rdesktop client, which allows connection to Microsoft Windows servers using the RDP protocol.
    - SSH — the OpenSSH secure shell client, used for remote command line access to host computers.
  - The Utilities folder contains various utility programs:
    - xPDF — a PDF file viewer.
    - mtPaint — a graphics file editor.
    - Image Viewer — the gpicview image viewer.
    - Text Editor — the Leafpad text editor.
    - SCRx31 Firmware — a utility for updating SCM reader firmware.
    - Display Size and NVIDIA Display Settings — same as on the desktop.
  - The Shutdown folder contains options to Shutdown and Reboot the computer.
  - The Settings folder contains any configuration settings:

- Focus — changes the behavior of when windows become active. Selecting ‘Click to focus’ means the user has to click on a window to make it active, selecting ‘Sloppy mouse focus’ means the window becomes active as soon as the mouse enters the window (no clicking necessary), and selecting ‘Custom’ does the same thing as ‘Click to focus’.
- The Quick Launch area contains icons for frequently-used productivity aids:
  - Show Desktop — hides any active windows and shows the desktop.
  - Xterm — a command line program providing local shell access.
- The Open Programs area shows any running programs or open windows. This area is empty if no programs are running and no windows are open.
- The Status area shows important system status indicators:
  - The Wicd Network Manager icon, which serves multiple purposes:
    - The color shows network status (green = connected, black = disconnected)
    - Hovering over the icon shows the currently-assigned IP address
    - Clicking on the icon opens the wicd Network Manager utility
  - The system clock.



**Figure 9 — LPS-Public Deluxe Desktop**

## 4.2 Connecting to the Network

LPS supports wired and wireless (WiFi) networking, but not dialup or cellular broadband wireless networking. We recommend using LPS with wired or wireless networking using DHCP. Setting static addresses requires root (admin) level access, which is present by default but which may be disabled in some distributions. LPS does not preserve user configuration data across reboots, so any static addressing information will have to be re-entered every time it is used. Likewise, wireless keys will also not be preserved.

### Using Static Addresses

It is possible to configure your computer to use a static IP address, but that requires some extra effort (as well as root-level access, which is available by default but which may not be present in all LPS distributions). Use the Wicd Network Manager to set the static IP settings, as shown in Figure 10. Click on the Properties button for the Wired Network connection, check the box for “Use Static IPs”, and enter the appropriate information (IP address, netmask, and gateway). Check the box for “Use Static DNS” and enter the appropriate data if you must supply your DNS server addresses manually.

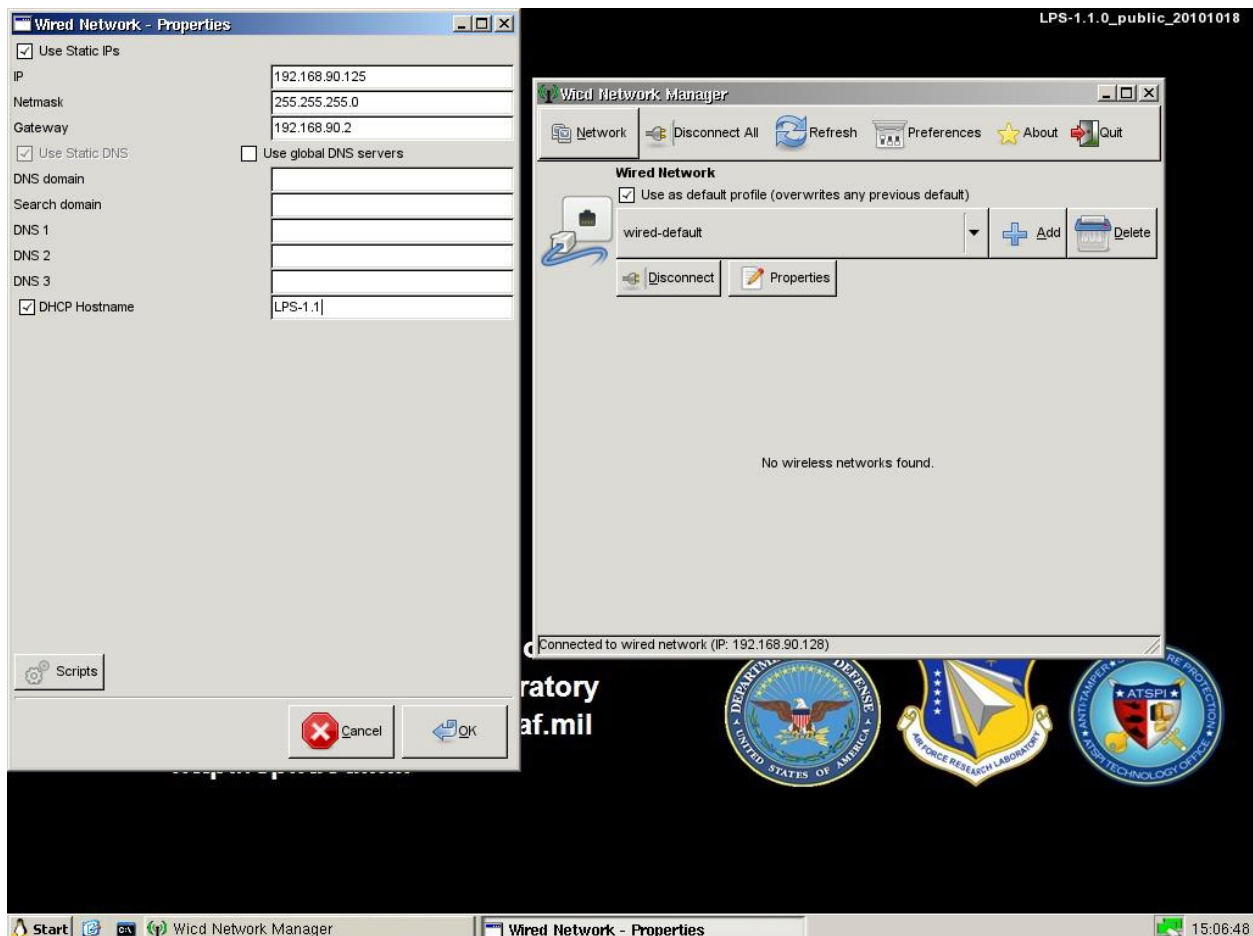


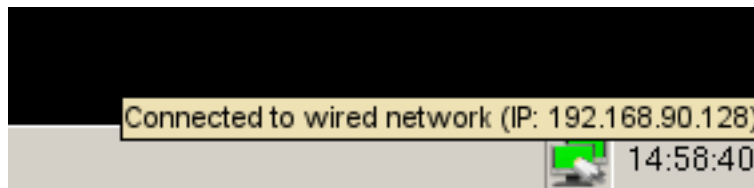
Figure 10 — Setting Static IP Address

## Using Wired Networks

If you connected your computer to a wired network port when LPS was booted, your computer should have had an IP address assigned automatically by DHCP. If not, unplug your connection and re-insert your network cable to get a new address assigned. You can tell you are connected by observing the Network Manager icon in the status bar; it should be green (see Figure 11). Hovering your mouse over the icon should show you a valid IP address for your network (see Figure 12). The Wicd Network Manager also has a display area within the application; it should also confirm that you are connected to a wired network and show the IP address (see Figure 13).



**Figure 11 — Network Manager Icon: Connected**



**Figure 12 — Network Manager Icon: Hover to Show IP Address**



**Figure 13 — Network Manager Status Display: Connected**

## Using Wireless Networks

If you intend to use wireless networking, start by opening the Wicd Network Manager. You should see a list of available wireless networks detectable by your computer (see Figure 14). If not, click on the 'Refresh' button at the top of the screen. If you need to connect to a hidden network, click on the 'Network' button and then select 'Find a hidden network' as shown in Figure 15. You will be prompted to enter the ESSID (network name) of the network, and it will then appear in your list of available networks.

The network display will be sorted in decreasing order of network signal strength. The display will show the network name, the signal strength, the type of encryption used (if any), and the network channel. An open network will show as 'Unsecured'. To connect to an open network, simply click the 'Connect' button for that network.



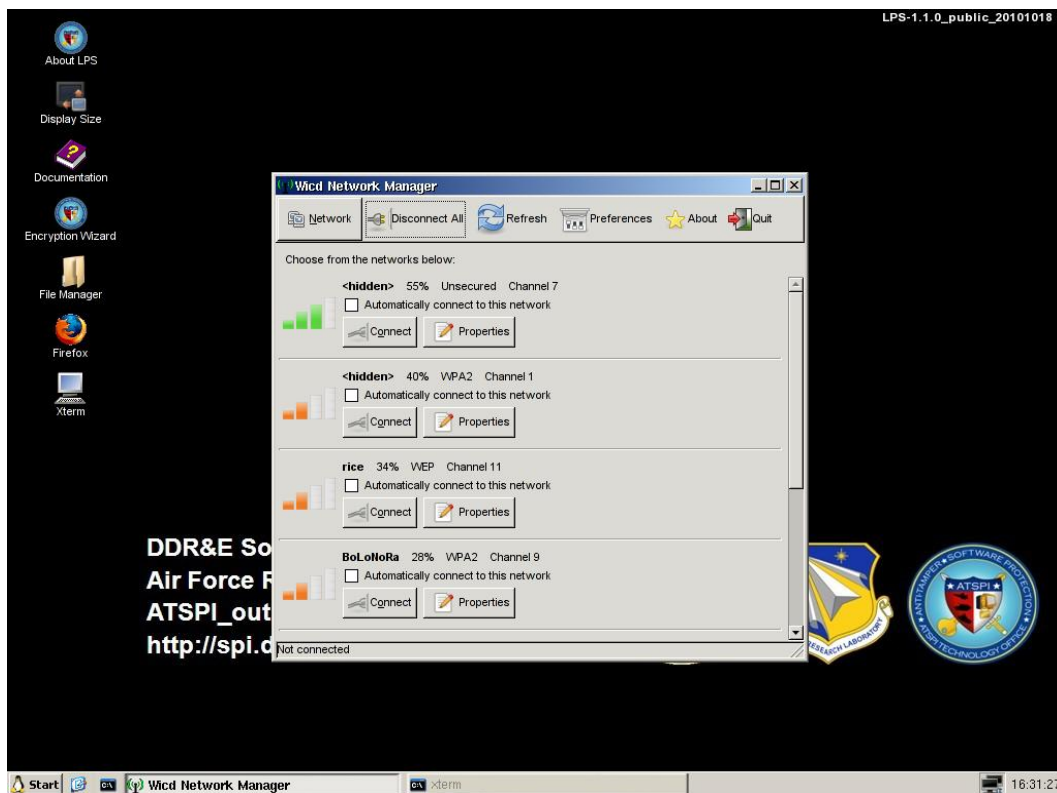


Figure 14 — Using Wireless Networks

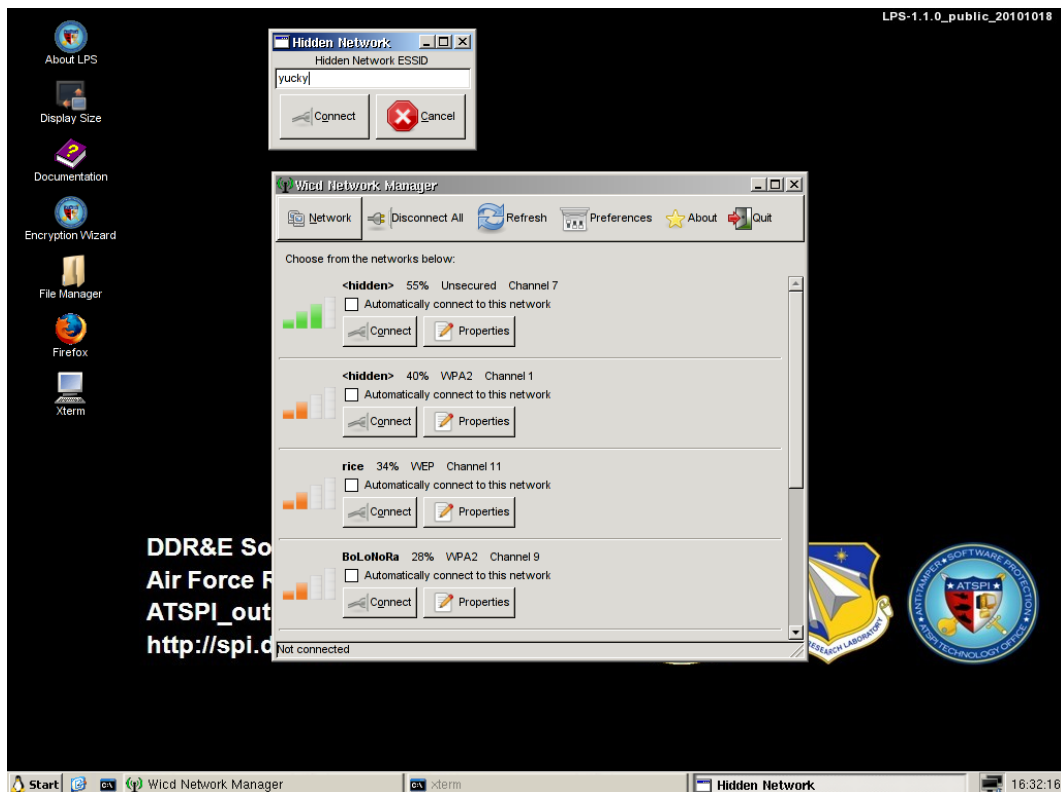


Figure 15 — Connecting to a Hidden Wireless Network

To connect to a secured network, additional steps must be taken. Click on the ‘Properties’ button of the network, which will display the Properties page (see Figure 16). Static IPs and DNS servers can be set (as with wired networking), but the most important option is to check the ‘Use Encryption’ box, select the appropriate encryption protocol (WPA, WEP, etc.), and then enter the network key. Depending on the type of encryption used, the key may be a hex string, a passphrase, or something more complicated. Most home and hotel networks will either be unsecured (not a recommended solution) or will use WEP or WPA. WPA2-Personal is the more secure option currently, but not all home devices support this protocol.

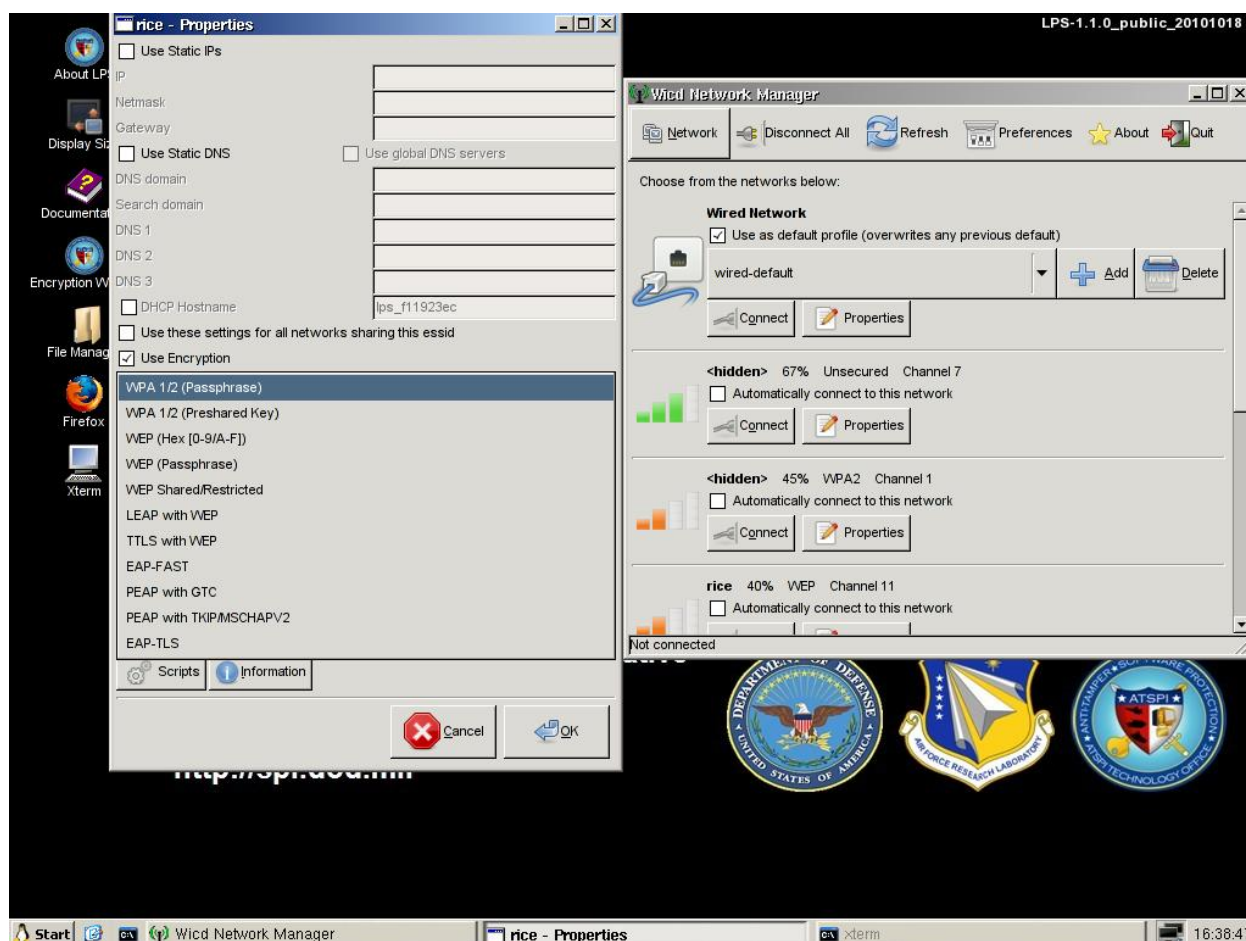


Figure 16 — Wireless Connection Properties Page

### 4.3 Browsing the Internet

Use the Wicd Network Manager to initially verify connectivity; the status icon should be green, and an IP address should be assigned. Start up the Firefox web browser and test basic network connectivity. Browse to a public website like [www.google.com](http://www.google.com). If you are accessing the network from a hotel or other public location, there may be intermediate network access screens to navigate. For example, some hotels and public Internet cafes require entering codes or acknowledging licensing agreements before granting access to the public Internet. If your networking does not work properly, see the troubleshooting discussion in Section 5.

The standard LPS-Public distribution includes the Firefox web browser. Starting the Firefox application should be sufficient to start browsing the public Internet. Some custom LPS distributions may have the default browser removed. In that case, connect to a corporate network using a VPN, remote desktop or terminal server application and browse from within the target network.

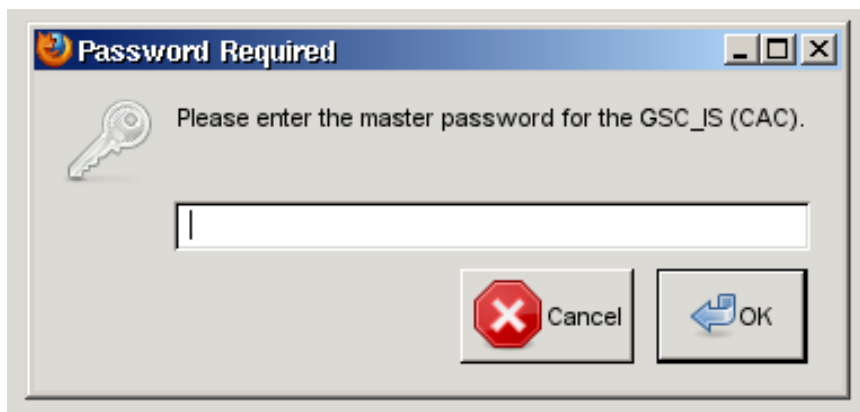
Once basic network connectivity is verified, you can use LPS applications to connect to private networks using a variety of protocols. LPS can support several different methods, and not all may be present in your specific LPS distribution. Check with your network administrators or computer support staff to determine the best method for connecting to your private network.

LPS doesn't impose any restrictions on what sites you can visit, but it also won't bypass any firewall rules, proxy servers, or other filtering and control restrictions in place on whatever network you are using. Some organizations have corporate policies blocking access to certain websites from within their networks. In that case, the browsing experience could be different when connected to the corporate network than when using the browser directly within LPS.

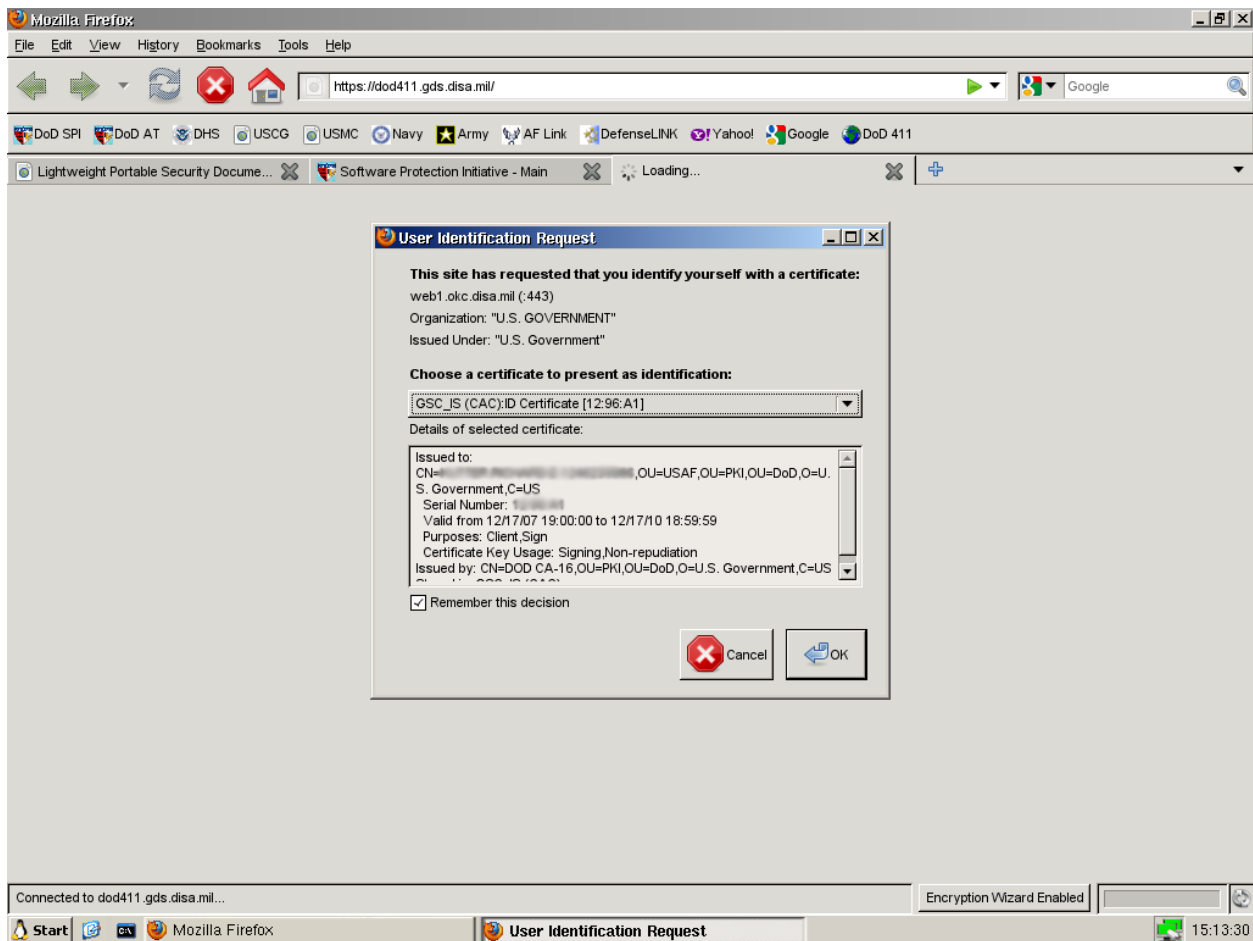
## 4.4 Using a CAC or PIV

Government users in the DoD are familiar with using the Common Access Card (CAC) to authenticate to computer systems. Other US Government users are familiar with using the Personal Identity Verification (PIV) card for the same purpose. LPS supports using an external USB SmartCard reader, but not many internal readers. Make sure the SmartCard reader is connected to the computer and be sure the CAC/PIV is inserted before launching the web browser. This allows the use of CAC- and PIV-enabled websites.

If you access a CAC- or PIV-enabled website, you will be prompted for a password (the Password Required dialog box—See Figure 17). It requests a Master Password, which is simply your PIN. CACs and PIVs typically have multiple certificates loaded. In the User Identification Request dialog box, you will be prompted to select the appropriate certificate. Choose a certificate from the drop-down list—it is typically the ID certificate on the CAC/PIV, although some web applications, particularly Outlook Web Access (OWA), can use the Email Signature certificate for validation (see Figure 18). Subsequent web pages and application may request further authentication (either CAC/PIV or username/password). Continue to supply your PIN or credentials when requested.



**Figure 17 — CAC PIN Request from Firefox**



**Figure 18 — Certificate Selection**

## 4.5 Connecting to Email and Using Remote Systems

You may have several different email accounts—from corporate to personal—that you want to access while running LPS. The experience will vary based on specific customizations within LPS, but the standard distribution will allow you to check private email (e.g., gmail) via a web interface, corporate email via a web portal, corporate email via remote desktop services, and potentially host-based email via ssh.

To connect to email, you first have to understand where the system is running. If you are using a web-based commercial service, then simply connect to the Internet, start Firefox, and connect to your email service. Supplying typical username and password credentials will give you access, and all operations are performed from within the browser.

If you are using a corporate or private email solution, then you will have to determine whether you are connecting to it via a web portal or via remote desktop services. A private email system will often support both interfaces. To use a web portal (e.g., OWA), you will have to establish a secure web connection (https: not http:) to a webmail server. Your email administrators will provide you with the URL for the server, and any login instructions. Authenticating to most US Government email services requires the use of a CAC or PIV card; other solutions may require a

simple username and password. Once connected, you will use a web browser interface to access your email.

Another popular solution for corporate or private email systems is to use a remote desktop or application virtualization solution (e.g., Citrix) to access either a full desktop or an application on a remote system. In the full remote desktop solution, the client presents a virtual desktop that is running on the corporate or private network. Screen images, not data, are being transferred between the client and the server. The server is manipulating the data on the private network on your behalf. Once in a familiar desktop, you can run a variety of applications including an email client (e.g., Outlook). This solution is popular since it presents a familiar interface and uses the same software as would be used if you were directly running on the private network. Application virtualization is similar, except a specific application is presented rather than a full desktop. Running the email client as an application would give you the same email experience as from the desktop virtualization solution, except that you wouldn't be able to run other applications.

Some people using host-based email solutions might use ssh to access the remote system. Supplying a network address and credentials allows host-based access where email applications can be run. Similarly, remote desktop software allows access to other systems where applications can be run, but are generally done within the same network.

## 4.6 Working with External Storage

By design, internal storage devices are not supported by LPS; this prevents any malware from being stored and from interfering with subsequent operations. LPS-Public supports the use of external storage devices (e.g., USB hard drives and flash drives). This functionality may be removed in some custom versions of LPS.

LPS-Public can boot from a USB flash drive. If it does, the boot stick will be unmounted after LPS loads. If the stick is unplugged and then re-inserted, it can be used to store files. However, we recommend that you use separate boot and data flash sticks to protect your boot device from contamination. If you use LPS on a flash stick in the same way as on a CD (i.e., separating your boot device from your data storage device), you will be operating in a more secure manner.

You can connect external storage device to your computer before or after booting the system. LPS will recognize devices being connected and will mount them automatically. When you insert a USB device, an icon will show up on the desktop called "USB Device [sda1]" (see Figure 19. You can double-click on this icon to browse files on the device using the File Manager, as shown in Figure 20.

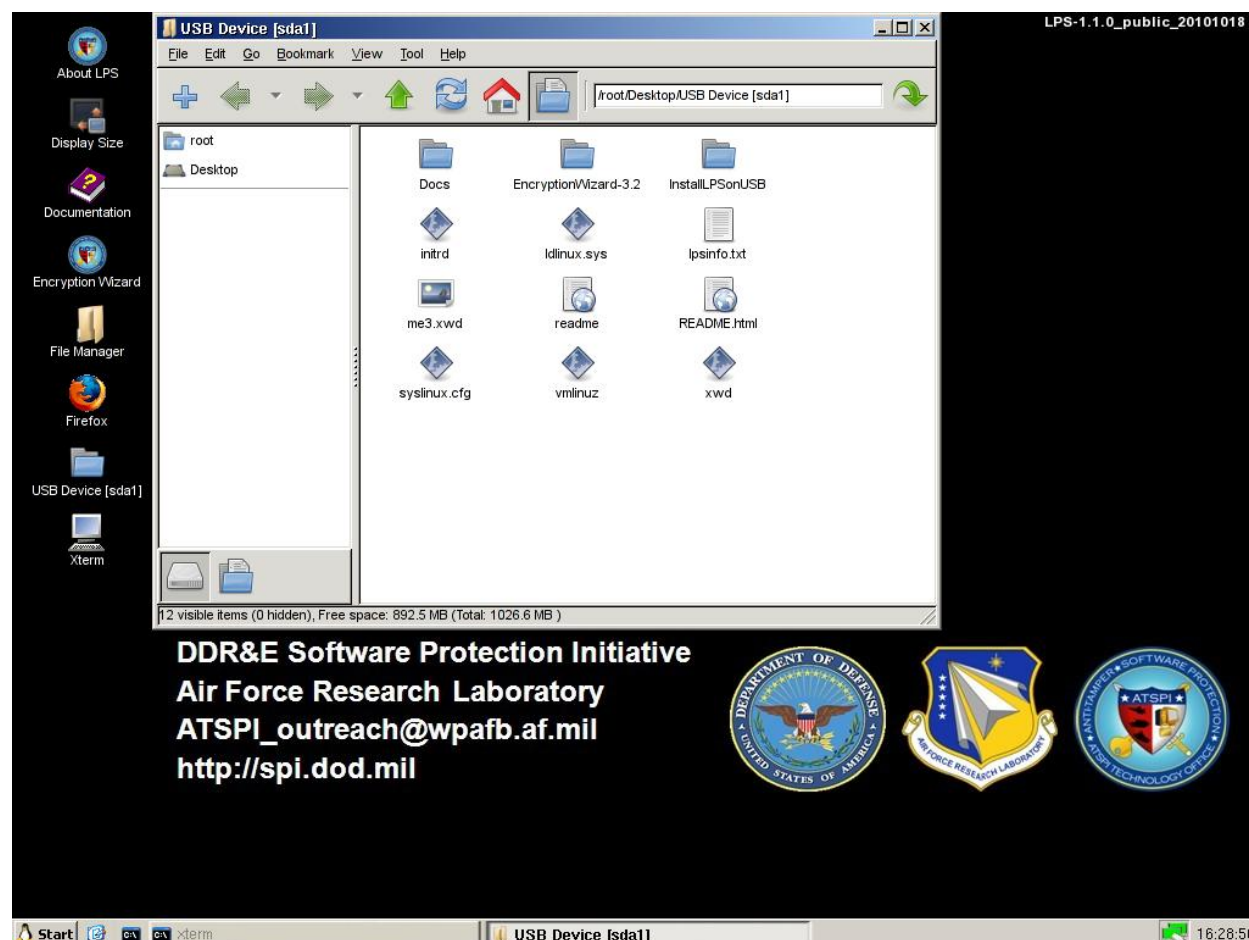


**Figure 19 — USB Device Mounted on Desktop**

External USB devices are mounted in the Linux file system under **/mnt/usbdevice** as **sda1**, **sdb1**, **sdc1**, etc. You can browse these volumes using the File Manager, the Xterm command line, or the Open and Save dialog boxes of applications such as xPDF or Open Office in LPS-Public Deluxe.

If you unplug a USB device, the USB Device icon will disappear from the desktop. Be sure you have closed all files on the drive and allowed all write operations to complete. Some devices have a status indicator light; wait for it to stop flashing before removing the flash stick. For maximum safety, do not disconnect the external storage device until the computer is shut down.

LPS only supports FAT-formatted storage devices as read-write drives. LPS can mount an NTFS-formatted device, but will only use it as a read-only drive.



**Figure 20 — USB Device Opened in File Manager**

## 4.7 Encrypting Data

### Using Encryption Wizard

The standard LPS distribution contains ATSPI's Encryption Wizard software. Encryption Wizard is a Java-based file encryption program that can be used to quickly and easily encrypt sensitive (but not classified) files for local storage and before transmission via email. It provides



a graphical user interface and uses strong encryption. Note that this feature may be removed in some LPS distributions.

Encryption Wizard can use shared passphrases, PKI certificates, or both to encrypt files. An encryption wizard file has a .wzd extension, and can be attached to an email message. When sending an encrypted file to another user, you can use their public certificate to encrypt it. DoD users can obtain certificates in three ways:

1. Download the public certificates of anyone with whom you will be communicating. You can use <https://dod411.gds.disa.mil/> to download certificates.
  - Authenticate to the site using your CAC.
  - Find the person with which you intend to exchange encrypted emails by searching.
  - Note their email address; you must use this address to send mail.
  - Click on the last name link.
  - Click on the link to download a .cer file for non-Outlook users.
  - Click on the link to download a Hardware (CAC) certificate.
  - Save this certificate to your root drive, or to an external data stick.
2. You can use Outlook within Windows to save public certificates for use later in LPS. In Outlook (connected to a Microsoft Exchange server, not offline), use the following steps:
  - Open Contacts.
  - Search address books (find in global address list) for your recipient.
  - Right-click the recipient, then select Add to Contacts.
  - Click on the Certificates icon in the menu bar.
  - Click on the Export... button to save the certificate file.
  - Cancel creating the contact (no contact is actually saved if you stop at this point).
3. Encryption Wizard can be used to obtain your public key to share with others. Use Tools, Export CAC certificate to create a .cer file. This key can be given to others with whom you will be communicating. You can also ask others to send you their key this way as well.

See the Encryption Wizard User's Guide in the LPS online documentation for more details about using Encryption Wizard.

### **Using Outlook Web Access**

Users wishing to encrypt data in email using Microsoft's Outlook Web Access (OWA) should note that OWA does not support S/MIME properly on Linux platforms or in non-Microsoft browsers. OWA users cannot sign or encrypt emails, although they can read signed emails. We are investigating solutions, but in the interim, Encryption Wizard can be used to encrypt message content and transmit it over government email systems. Both the sender and the recipient need to have Encryption Wizard on their systems, and they need to agree on a passphrase for encryption and decryption (or use public keys, as described above).

## Using Gmail

A partial workaround for sending and receiving encrypted emails exists using the Gmail S/MIME add-on. The process is somewhat complicated, and does require some setup to work properly. Follow these steps to send and receive encrypted email:

- Obtain a free Gmail account.
- Obtain the public certificates of anyone with whom you will be communicating (see alternatives under discussion of Encryption Wizard).
- Add the certificates to Firefox.
  - Edit, Preferences.
  - Advanced tab.
  - View Certificates button.
  - People tab.
  - Import... button.
  - Select the certificate(s) you saved previously, then click OK.
- Use Gmail via the web interface to send or receive mail.
  - Click on 'Compose Mail'
  - Enter the email address of the recipient (noted above)
  - Click on the 'sign' or 'encrypt' icons as you wish (highlighted in Figure 21).
  - Send the message.
  - When prompted for your certificate, choose your Email Signature Certificate for signing.
  - Enter your CAC/PIV pin when prompted for a master password.
  - Enter your Gmail password when prompted.

### Usage Notes:

- You cannot add your own certificate as a recipient within Firefox.
- You must use the same email address for the recipient as contained in the certificate.
- You cannot forward an encrypted message from OWA to Gmail and be able to decrypt it.
- Outlook users can send encrypted messages to LPS users on Gmail if they use *both* the Outlook address and the Gmail address on the original message. Outlook will complain about not having a certificate for the Gmail user, but ignore the warning and tell Outlook to send the mail anyway. The Gmail user will be able to use a CAC/PIV to decrypt the message as long as they are using the same certificate as the Outlook recipient.

For users needing to electronically sign emails, we offer a workaround using the Gmail S/MIME add-on. Users with a Gmail account can sign emails using their CAC/PIV and send them to recipients on a government email system. Compose the message in Gmail, click on the sign icon (see Figure 21), use your CAC/PIV to sign, and then send the email. Signing messages works



with or without encrypting them. Recipients using Outlook (but not OWA) will be able to verify your signature.

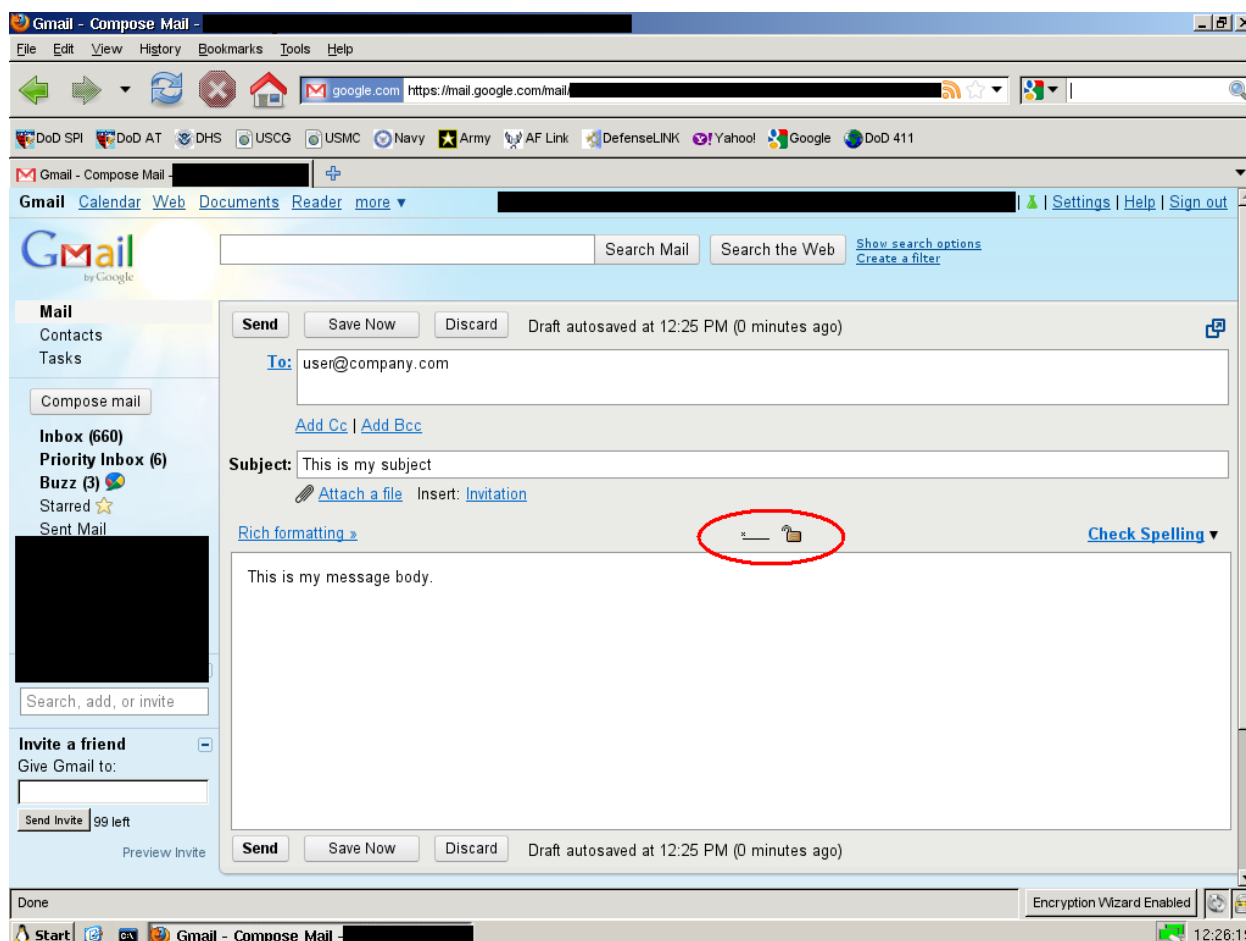


Figure 21 — Gmail S/MIME Sign and Encrypt Icons

## 4.8 Create your own bootable LPS USB Flash Stick

The LPS CD should contain a directory called **InstallLPSONUSB**. While booted into Windows (not LPS), connect a new USB flash stick to your computer and note its drive letter. Next, run the *LPStoUSB* batch file in the InstallLPSONUSB directory. Follow the prompts and it should install LPS on the flash stick.

Caveats for creating your own LPS on USB:

1. Allow the batch file to format the flash stick. This process prepares the flash stick for use as a boot device; otherwise, it may not boot.
2. The installation script requires admin rights. Under Windows XP, you must be logged in as a member of the Administrators group. Under Vista or Windows 7, this means the command line process where you run the *LPStoUSB.bat* file must have administrator rights. You can do this by:
  - a. Logging in as an administrator with User Account Control (UAC) disabled

- b. Logging in as an administrator with UAC on, but run the command line as an administrator. [Start, Programs, Accessories, right-click on Command Prompt, Run as Administrator]
  - c. Logging in as a normal user, but run the command line as administrator as in (b).
- 3. USB devices and ports are rated at different speeds. Faster ones can boot in less than a minute. Slower ones will take longer, but are usually faster than CDs.

## 5 Troubleshooting

**Check the Frequently Asked Questions (FAQ) in the online documentation before requesting help.**

**If you are using a customized LPS build for your organization, contact your organization's computer support help desk first.**

Users with a limited amount of computer skills can still do rudimentary troubleshooting. The following scenarios cover common problems and potential solutions.

### 5.1 Can't Boot from CD

Make sure the CD-ROM drive is recognized by the computer. You can verify this by browsing the CD after booting your home operating system.

If you are using a Mac, make sure you are holding down the “c” key while booting the computer. Alternatively, you can hold down the *option* key while booting to be presented with a list of bootable devices—select the CD-ROM drive. If these methods don't work, boot the Mac normally, then open the System Preferences utility in the Applications folder. Select Startup Disk, then choose the CD—it may show up as “Foreign OS on CDROM”. Restart the Mac. Changing boot devices requires admin credentials.

If you are using a PC, you need to make sure that your computer's BIOS is configured properly. It needs to be set to boot from the CD-ROM drive before the main hard drive, or the CD should be chosen as the boot option from the one-time boot screen.

Follow these steps to troubleshoot a PC:

- Reboot the computer and enter the hardware setup screen. This usually involves pressing certain key(s) during a specific part of the boot process. The specific keys vary by hardware manufacturer and model. The keys are sometimes displayed on the screen during the boot process, and are often a function key (e.g., F1, F10, F12). If the operating system on the computer's hard drive starts to load, you missed the interval where the key can be pressed. Restart and try again.
- Your computer may have a password-protected hardware setup screen. If so, request that your computer support technicians configure your system for you.
- Once you have accessed the hardware setup screen (which may look similar to the screen shown in Figure 22), configure the boot order so that the computer boots from the CD *before* the main hard drive or select the CD from the one-time boot screen.

Regardless if you are using a Mac or a PC, if you have reached this point and LPS still isn't booting, it is possible that your LPS disc is damaged. Try to boot LPS on a different computer. If that doesn't work, contact your organization's help desk to request a replacement disc, or download the latest image from the SPI web site and burn it to a new CD.

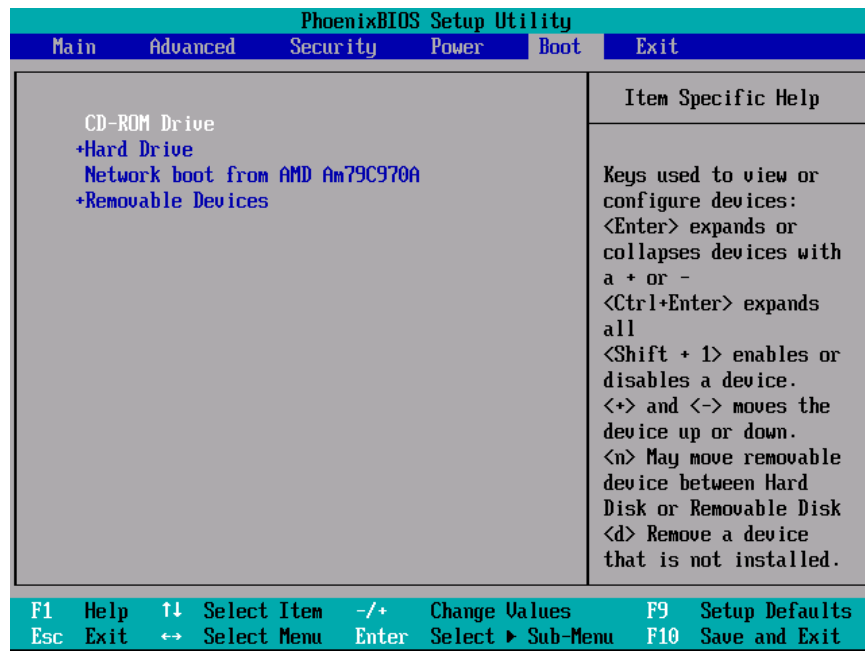


Figure 22 — BIOS Setup Screen

## 5.2 Hangs During Booting

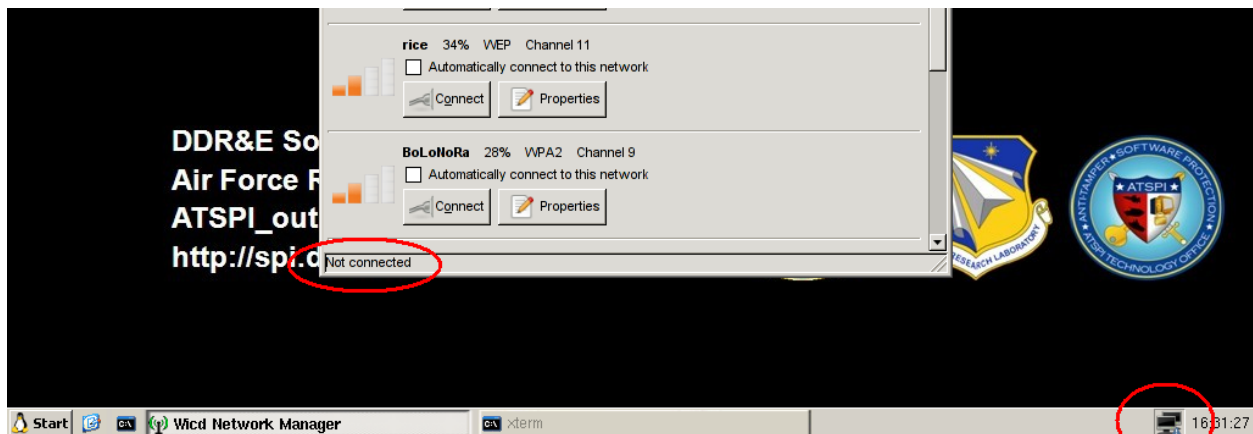
If LPS shows the startup screen (dots marching across the screen), the splash screen (graphical screen showing a progress indicator), but then hangs without starting the desktop (the screen with the icons), then the most likely problem is a video driver incompatibility.

Please contact the ATSPI Technology Office with the brand and model of your computer and the type of video card/chip present in your system. We will attempt to find a compatible driver and include it in a future maintenance release.

## 5.3 Can't Access the Network

LPS runs health checks when booting to ensure a network driver is available for your hardware devices. If this script detects an error condition, a warning screen will be displayed as shown in Figure 4. It usually means that a physical device is present, but LPS does not have a driver for it. You may still be able to use a wireless connection, but please report this error to us so we can add the necessary driver in a future release.

During the LPS boot process, you can observe progress using the startup screen's verbose message display (press F2). A lengthy pause while in the section called Configuring and Starting Network usually indicates failure. Once you reach the LPS Desktop, you can confirm your lack of connectivity by opening the Wicd Network Manager and looking for the status indicators highlighted in Figure 23.



**Figure 23 — Two Indicators of Lack of Connectivity**

If you did not receive a warning screen during startup, your computer has a recognized Ethernet controller with a valid driver. You should still check for connectivity (see Figure 23) to see if you have a live connection with a valid IP address. If you don't intend to use wired networking, you should use the Wicd Network Manager to connect to a wireless network. If you don't have a recognized wireless controller, please let us know the manufacturer and model so we can add a driver in the future.

If you did not receive a network error message, but you want to use wired networking, then you should start troubleshooting your network connection starting first with the network interface in your computer. Make sure you have a wired network interface in your computer and that it is enabled and working properly. Some computers allow devices to be disabled in the hardware setup. Reboot the system into your home operating system (on your internal hard drive) and test the network connection.

A problem with the network device or the lack of a necessary driver is unlikely to be resolved quickly, and usually represents an unrecoverable error. If there is a physical error with the network device, it will likely have to be replaced. If the network interface is not supported by LPS, then a trouble ticket will have to be opened to log the problem.

If the network interface is functioning properly, then you will have to check your network connection and make sure network services are functioning properly. This error exists if your computer does not get a valid network address assigned. This is a much more common error, and usually indicates a basic connectivity problem. Try the following steps to troubleshoot the error:

- Check the physical connection. If using a wired connection, is your computer plugged into the network? Do you know that your cable works properly? Is the network port you are connecting to operational? If using a wireless connection, is your wireless access point functioning properly, and is it connected to the upstream network?
- Make sure you are using a wired or wireless connection and not dialup or wireless broadband—LPS does not support those connectivity options in this version.
- Be sure you plug in the network *before* you boot into LPS. After you boot LPS, you may have to unplug and reinsert the network cable to get a new address assigned, or use the Wicd Network Manager to disconnect and reconnect to a network.

- Check that DHCP services are available and are functioning properly. You know that it works by seeing that an IP address has been assigned. Use the Wicd Network Manager to check your IP address, or hover your mouse over the Wicd Network Manager status icon.
- Boot the computer into your home operating system from your local hard drive. Check that network connectivity works properly. For example, boot your computer into Windows and check network connectivity using Windows-based applications and tools.
- Make sure the DHCP service is available and assigning addresses. This is best tested using your home operating system.

## 5.4 Can't Access Local Drives

Make sure that your distribution supports local drive access. By default, LPS-Public supports USB-connected devices (hard drives, flash devices, etc.). However, some custom distributions might remove this capability. If you are running a custom distribution, check that USB device support is present. Starting with version 1.1.0, LPS displays an icon on the desktop for each mounted volume (see Figure 19).

The internal hard drive of the computer will never be accessible—this is by design. No drivers are present for using the internal hard drive.

Unplug and reinsert the external device. Make sure it is powered on (if it contains external power). Most USB devices are powered directly by the computer. Depending on the device, there may be a status light that shows that power is being received and that the device is communicating with the computer.

Check how the external device is formatted. LPS only works with FAT-formatted volumes. NTFS volumes should mount, but will be read-only.

## 5.5 Can't use a CAC/PIV

To troubleshoot this problem, make sure there is a SmartCard reader attached to the computer and that it functions properly. Verify the following:

- Make sure you are using an external USB-connected SmartCard reader. Some computers have built-in readers—the drivers for many of these devices are not loaded in LPS.
- Make sure the SmartCard reader was connected to a USB port of the computer *before* launching Firefox.
- Once booted into LPS, open a command window using **xterm** and check that the SmartCard reader is recognized by the computer. Type *lsusb* and look at the list of devices present. You should see something like “SCM Microsystems, Inc. SCR331 SmartCard Reader” listed. If you do not see any devices listed, then the hardware is not recognized by LPS.
- Try connecting the SmartCard reader to another USB port. Verify that the reader works on another computer.
- Check that you are running the most current version of firmware for your SmartCard reader. Older versions of readers may have outdated firmware; CCID-standard firmware

is required. If you have an SCM Micro SmartCard reader, a Firmware Update utility is included in LPS. Follow this procedure to update your reader:

- Open the Utilities folder from your start menu.
- Run the *FirmwareUpdate* utility.
- Read the instruction screen, click the *Continue* button.
- The **FwUpdate** utility opens. Click the *Browse* button.
- Select the latest bin file (e.g., SCR531\_V525.bin). Click the *OK* button.
- The **Reader** field should show your CAC reader. Compare the **Firmware Ver** field in the **Current Firmware** column against the **New Firmware** column. If the **Current Firmware** version is lower than the **New Firmware** version, click the *Download* button to update your firmware with the new software. Otherwise, click the *Cancel* button to exit.
- The progress bar should show “Downloading...” then “Verifying...” as the progress indicator moves towards completion. Once finished, the status area should display “Download Success.” Click the *Close* button to exit the utility.

Reboot into LPS and try to use the SmartCard reader again.

If your computer recognizes the reader, but does not seem to recognize that a CAC or PIV is inserted, check the following:

- Check that the CAC/PIV is recognized in the SmartCard reader. Readers will often use LED lights as a status indicator; look for a status change. For example, on the SCM SCR331 a blinking green light indicates normal operation, but a solid green light means the card cannot be read. Try removing and reinserting the card. Try cleaning the card with a soft, damp cloth and drying completely before using. If that doesn’t work, then shut down the computer, remove and reinsert the reader, reboot, and reinsert the card.
- Check that the card was inserted before accessing a CAC- or PIV-enabled website. If you forget to insert the card first, insert the card, restart the web browser, and try accessing the website again.

If your SmartCard reader and CAC/PIV are working properly, you still may experience some operational issues while using the system. Be aware of the following conditions:

- When you are prompted for a Master Password while using your CAC/PIV, remember that this is your PIN. You do not need another password.
- Make sure you are using the correct certificate. Not all web sites use the same certificate, and some will use the Email Signature certificate for authentication.
- NOTE: If you enter an incorrect PIN for your CAC/PIV three times in a row, you may need to have it reset at your organizational CAC or PIV PIN reset station.

## 5.6 No Sound or Printing

This is intentional. No sound or print drivers are included in this version of LPS. Sound and printing are planned for inclusion in a future release.

## 6 Support

### 6.1 Warranty

LPS-Public is Government-Off-The-Shelf software, and is supplied as-is with no warranty implied.

### 6.2 License

LPS-Public uses free software components under the GNU Public License (GPL). The standard LPS software can be freely distributed without restriction.

Some custom distributions may include licensed software products (client access components, etc.). LPS does not confer additional licensing terms beyond those of the underlying products. In all cases, licensed software is included in a distribution for a specific organization. That organization is responsible for managing client access licenses, enterprise agreements, or other licensing vehicles, and for ensuring that all users receiving a custom LPS distribution are properly licensed for any third-party software included.

You are only granted a license to use the software after you have agreed to the following: You will indemnify and hold harmless the author, owner and distributor of the LPS against any and all liability, claims, suits, losses, costs and legal fees caused by, arising out of, or resulting from any negligent, reckless or willful act by you, or from any omission or failure to act by you. You will indemnify and hold harmless the author, owner and distributor of the LPS against any and all liability, claims, suits, losses, costs and legal fees caused by, arising out of, or resulting from any negligent, reckless or willful act by anyone accessing the LPS distribution through you, or any omission or failure to act by anyone accessing the LPS distribution through you. You will make any further distribution of the LPS, if permissible, contingent upon the distributee agreeing to all license terms and conditions.

Please see the software distribution for other possible license terms.

### 6.3 Contacts

If issued a custom build of LPS by your organization, contact your normal first-line computer support for problems using LPS. These support teams will have escalation contacts for second-level support. Home users may contact the ATSPI Technology Office directly.

The ATSPI Technology Office provides third-level support and custom development, and handles feature requests (such as supporting additional hardware devices or adding custom applications).

#### **ATSPI Technology Office**

Air Force Research Laboratory, Sensors Directorate

AFRL/Rywa

2241 Avionics Circle, Bldg 620

Wright-Patterson AFB, OH 45433-7320

<http://spi.dod.mil>

[ATSPI\\_Outreach@wpafb.af.mil](mailto:ATSPI_Outreach@wpafb.af.mil)